SOCIAL NETWORK FORENSICS

Shivam Kapil, Ashwini Kumar, Rishav Bansal, Nancy Victor

School of Information Technology and Engineering, VIT University, Vellore.

Email: shivam.kapil2016@vitstudent.ac.in

Received on 25-10-2016

Accepted on 02-11-2016

Abstract

As we know, there are more than 1.72 billion active users of Facebook, forensics data collection on social network has become an important research issue. Social network is like a treasure trove for forensics investigation. Only social network implies that each user communication is saved entirely to the service provider, without direct access of the investigator. Here, we are going to help our cyber-crime department with the help of important data and analytical method. And we will show how these data can help the cyber-crime experts without the help of social networking operator. We will demonstrate the effectiveness of the algorithm by simulating the tracking of a person in a sandbox environment. The algorithm will work by mapping the activity of person to be tracked and the activities (people he is in contact with, pages he visits, times when he stays online etc.) will then be made into a graph. This paper also explains how to increase the security level of a Facebook id so that it cannot be hacked.

Keywords: Online network forensics, visualization, graph and social network.

1. Introduction

With the expanding utilization of informal communities and the develop of cloud computing, the number of users of these services increases steadily, with e.g. Facebook at this time claiming to have 1.72 billion consumers [1]. As long as conventional legal sciences depends on the physical procurement of equipment [4, 5] and the utilization of hash sums to guarantee prove unwavering quality, this way does not measures to cloud administrations and utilization of conveyed data hubs. The absence of institutionalized crime scene investigation APIs and in addition unified forms for administration administrators, confined arrangements are still in far reaching use. Another essential part of crime scene investigation is the correct representation of information [8, 6] because of the immeasurable measure of accessible information. It is besides difficult to picture assembled informal communication information in a way that can answer basic inquiries of enthusiasm on a rst locate, so that individuals without specialized foundation can
comprehend it. In any case, the consolidated. DB issue got across the board consideration with the arrival of the iPhone Tracker programming [3] in April 2011, which visualized. This has been appeared for instance on account of the consolidated. DB from iPhone: the le includes geolocation data what has been as of now delineated in 2010 [7]. The gathered information. because of the iPhone Tracker programming, IPhone Company requires to survey and replace the information gathering method [1]. Here we distinguish information source of interest for measurable tests on informal communities, and how they are able to utilize in a robotized form. Moreover distinguish charts of intrigue that are able to produce from these information sources and able to answer numerous conceivable inquiries of a legal analyst on rest locate. According to the present situation, there is not yet any work on scientific examination of information from interpersonal organizations without the joint effort of the informal community administrator. We indicate case charts and show conceivable representations, which can and ought to be utilized for informal organization examination and will be discharged under an open source permit. The rest part of paper is as follows: Section 2 give information of the social networks and how they are were used earlier for solving crimes. Section 3 demonstrates what information can be removed from interpersonal organizations for interpersonal organization measurable examination, Section 4 clarifies the information and how it will be imagined. We demonstrate the plausibility of our approach in Section 5.

2. Literature Survey

Informal community crime scene investigation needs to depend on a constrained arrangement of information commencement in numerous conditions. Obtaining the server's data is not possible, and utilizing administration administrator's information straightforwardly requires the administration administrator's collaboration. On the off chance that by any stretch of the imagination, the specialist can submit application to the administrator and may or may not get all the pertinent information (e.g. written in the Facebook law enforcement rules distributed by the EFF ). This is inconsistency Arrange scientific systems like PyFlag and Xplico just can't see or get to all the information, as they are exclusively inactive. Our approach, then again, does not require the collaboration of the informal community administrator, and can guarantee these features because of the accessible way of our accumulation technique and instruments.

2.1 Data Obtaining

Earlier having the capacity to break down interpersonal organization information the information must be accumulated what's more, gained. While conventional criminological strategies can be utilized to remove ancient
rarities from nearby web browser reserve, various different methods are likely on the correspondence layer. These range from aloof sniping on the system to dynamic assaults like sniping on decoded WI s or in sequence with ARP on LANs.

As of late suggested companion in the center assault, which utilizes an outsider augmentation for the informal organization in blend with a conventional crawler segment, could be utilized also. Slithering still is restricted, as metadata and exact timestamps are definitely not appeared on website pages. These are just accessible through utilizing the interpersonal organization APIs, which augment the accessible information of the web interface. Despite the fact that it would be conceivable to utilize inactive signing on correspondence layer, in case any situations where a judge requested legitimate capture on the Internet association of a suspect, this way is constrained and also it would take a colossal measure of time for gathering data, and fulfillment is scarcely conceivable. Moreover, numerous interpersonal organizations or the likelihood to scramble information on correspondence layer by making use of HTTPS, interpretation detached assaults pointless.

While Facebook declared as of late that clients are currently ready to download all their expert le information, the information gave by our strategy is far unrivalled compared to the Facebook master download choice which needs e.g., critical metadata and is in this way not valuable for crime scene investigation. All in all, it is impractical for a client to download everything that is associated with his or her expert on the informal organization. Another fascinating element as of late declared is Facebook Course of events, which urges clients to never erase anything from the social organize, and to utilize it as a memorable document. This without a doubt is fascinating for scientific examinations, as the client is less inclined to erase information.

3. Proposed System

In this paper we are helping the cyber- crime expert with the help of Facebook API and R-studio. We are first connecting the users Facebook profile to the R-studio then with the help of secret app id we are creating graph of the time period. This will show the uses time schedule of using Facebook with the help of that graph we are checking when the accused/user is online, so that with that graph visualization we can track that person easily. As we know we can only track the person when then person is online so with the graph we can easily find that when the user comes online always. Then if we are not able to track that person then we are creating graph for user friend who always be in touch. With the help of message system or like option system. Then we can easily track the friend of accused person and after that we can easily track the accused person with the help of his/her friend.
4. Implementation

//register as a developer using the link:

Link: - http://developers.facebook.com/apps

Registration is needed now because we don’t have a legal permission to access any account. But if the permission can be obtained from cyber-crime expert, then the account can be accessed directly.

Step 1: install R studio

Step 2: install packages
install.packages("devtools")

library("devtools")

install.github("Rfacebook","Pablo_barbera",subdir="Rfacebook")

require("Rfacebook")

facebook_oauth<-facebookOAuth(app_id="……………",app_secret="……………….",extended_permission=TRUE)

//then we need to enter host address

Then,

save(facebook_oauth,fie="facebook_oauth")

load("facebook_oauth")

//Generate the graph with the help of id…

//time graph for user….

>plot(userinfo$appid, type="l",main="time",xlab="days",ylab="time",col="black")

//If the cyber-crime expert will not be able to find the accused with this time graph then, generate a graph for friends, who all are in the contact of the accused person…
With the help of this, the work of the cyber-crime expert will become easy.

To access the information of friends we need to make connection.

```ruby
Friend = user.client.get_connection(“username/me ”,”friends”)Friend.each do |friend|
  Sidekid::client.enqueue(job::importfriends,userid,friend[“id”])
  Job::importmutualfriends.perform_at(50,userid,friend[“id”])
```

// Draw the graph using Rgraphgviz package

And install pixmap package

Use add logo function to show picture.

```
// With this graph we can track friends of accused person to get information.
```

5. Conclusion

Interpersonal organizations and the distributed computing worldview will without a doubt change the way crime scene investigation examinations are done sooner rather than later. Here, we have identified important information sources in interpersonal organizations; how they can be lever- matured for investigation, and discussed about to what extend this is conceivable without the cooperation of the interpersonal organization administrator. We executed a proof-of-idea application for making social interconnection and social cooperation charts (with client associated, with the client cooperate frequently) in the light of Facebook to demonstrate the practicality of this approach, which we discharge as unclosed source programming. As the future work, all the social networking API's can be used to help crime investigating officer.

6. References


